




**COUNTY OF LOS ANGELES
DEPARTMENT OF AUDITOR-CONTROLLER**

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 525
LOS ANGELES, CALIFORNIA 90012-3873
PHONE: (213) 974-8301 FAX: (213) 626-5427

WENDY L. WATANABE
AUDITOR-CONTROLLER

May 13, 2013

TO: Marvin J. Southard, D.S.W., Director
Department of Mental Health

FROM: Wendy L. Watanabe 
Auditor-Controller

SUBJECT: **HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT
COMPLIANCE REVIEW – ENHANCED SPECIALIZED FOSTER CARE
PROGRAM, COMPTON OFFICE**

We have completed a Health Insurance Portability and Accountability Act (HIPAA) compliance review of the Department of Mental Health's (DMH) Enhanced Specialized Foster Care Program, Compton Office (ESFCPCO), a HIPAA covered program. Our review was prompted by prior findings of non-compliance during an unannounced site visit to ESFCPCO. This report details our findings and a recommendation for corrective action.

Background

On November 15, 2012, we conducted an unannounced visit to ESFCPCO as part of our program to ensure that the County's HIPAA covered programs and clinics are posting their Notice of Privacy Practices (NPP) in prominent patient locations, as required. We noted that ESFCPCO did not post the NPP as required. In addition, there was no facility manager present, and the assistant to the facility manager did not know where hard copies of the NPP were located, indicating a lack of management knowledge and accountability for core HIPAA requirements. These findings prompted a full HIPAA compliance review of ESFCPCO.

Our review evaluated ESFCPCO's compliance with the HIPAA Privacy Rule and DMH's HIPAA policies and procedures. We also used the *HIPAA Privacy Rule and Health Information Technology for Economic Clinical Health (HITECH) Act Audit Tool* in evaluating their compliance. DMH management is responsible for establishing and maintaining effective internal compliance with HIPAA regulations, and has oversight of the HIPAA program throughout their facilities. We considered DMH's internal controls over their compliance program, and the HIPAA Privacy Rule requirements that could

have a direct and material effect on ESFCPCO. At the request of ESFCPCO management, we discussed our findings with them on the day of the review.

Summary of Findings and Recommendations

Notice of Privacy Practices

The HIPAA Privacy Rule requires a covered entity with direct treatment relationships with patients to give the NPP to every patient no later than the date of first service delivery, and to make a good faith effort to obtain the patient's, or their representative's written acknowledgment of receipt of the notice. If the provider maintains an office or other physical site where health care is provided directly to patients, the provider must also post the notice in the facility in a clear and prominent location where patients are likely to see it, as well as make the notice available to those who ask for a copy.

Our follow-up review found that the facility posted the NPP in the waiting area, where patients and visitors are likely to see it. ESFCPCO management verified that all patients are given the NPP on their first service delivery date. We reviewed five randomly selected patient charts, and noted they all included the required acknowledgement of receipt.

While ESFCPCO was not in compliance with the NPP standards at the time of our unannounced site visit, the facility has addressed the deficiencies in this area, and was fully compliant at the time of this review.

Safeguards for Protected Health Information

A covered entity must have in place appropriate administrative, physical, and technical safeguards to protect the privacy of protected health information (PHI). A covered entity must reasonably safeguard PHI and electronic PHI, and prevent any disclosures that violate the Privacy Rule.

We reviewed the following DMH and ESFCPCO policies and procedures:

- DMH Policy Number 500.21, *Safeguards for Protected Health Information*, which establishes administrative, physical, and technical safeguards to protect the confidentiality of PHI.
- DMH Policy Number 302.14, *Networked Information Systems Usage*, which governs the use of information technology resources by DMH employees.
- ESFCPCO's *Medical Records Safeguarding and Security* policy, which addresses safeguarding and securing medical records.

- ESFCPCO's *Procedure on Securing Confidential Protected Health Information* policy, which establishes guidelines for field operations staff to safeguard PHI.

ESFCPCO management reported that the facility does not have its own front desk, since most services are provided in the field. When ESFCPCO patients come in for appointments, they check in with the Compton Family Mental Health Center's (CFMHC) front desk staff, as this is a shared waiting area. ESFCPCO staff escort patients to their appointments, after CFMHC staff notifies them of the patient's arrival.

ESFCPCO management also reported that their computers are protected by endpoint protection software, which blocks downloading of PHI or other data to portable storage devices. In addition, ESFCPCO computers are configured to prevent workforce members from saving PHI onto their hard drives.

During our review, we noted that workforce members store patient medical charts in locked cabinets near their work stations. ESFCPCO management told us that the cabinets are secured at all times, and access is restricted to ESFCPCO staff that pull and track medical charts. They also reported that patients and visitors do not have access to the locked cabinets. We verified that the cabinets were locked during our review, and we did not observe patients or visitors in the records storage area.

To the extent that we were able to review ESFCPCO's administrative, technical, and physical safeguards, the facility appears to be in compliance with these standards.

Training

ESFCPCO, as a HIPAA covered program, must train all members of its workforce on policies and procedures related to PHI as required by the HIPAA Privacy and Security Rules, to the extent necessary and appropriate for them to do their jobs. Workforce members include employees, volunteers, and trainees.

The DMH Human Resources Division is responsible for ensuring its workforce members are trained on HIPAA compliance, and the Department's HIPAA policies and procedures via the Learning Net. ESFCPCO management provides additional, role-based training for their workforce members.

Our review of ESFCPCO training records noted that ESFCPCO is in partial compliance with the training standards. Four (11%) of 36 workforce members have not completed the required HIPAA training. ESFCPCO reported that these workforce members received basic HIPAA training from their direct supervisors and the training coordinator, but did not complete the required online HIPAA training.

Recommendation

- 1. ESFCPCO management ensure that all workforce members complete the required HIPAA training.**

ESFCPCO's response indicates that they implemented our recommendation. To date, only two (5%) of 36 workforce members have not completed the required HIPAA training but they hope to achieve 100% compliance by May 31, 2013.

Complaint Process

A covered entity must provide a process for patients to complain about its policies and procedures. In addition, a covered entity must document all complaints received and their disposition, if any.

ESFCPCO management informed us that patient complaints are handled in accordance with DMH Policy Number 500.11, *HIPAA Privacy Complaints*. Patients are directed to contact the Program Head or the DMH Patients' Rights Office to file a complaint.

We observed that the Program Head's name and contact information are posted on the registration window in the patient waiting area to allow patients to express their concerns regarding treatment or privacy issues. In addition, the DMH NPP posted in the waiting area informs patients that they may file a complaint with the U.S. Department of Health and Human Services (HHS), the County's Chief HIPAA Privacy Officer (CHPO), or the DMH Patients' Rights Office. We also verified that HIPAA complaint forms were available in the waiting area. It appears that ESFCPCO complaint process complies with HIPAA standards.

Refraining from Intimidating or Retaliatory Acts

Discussions with ESFCPCO management confirm they are aware of their obligation to comply with DMH Policy Number 500.18, *Refraining from Retaliatory or Intimidating Acts Against Individuals That Assert Rights Under HIPAA*. They also understand that the Office for Civil Rights (OCR) will investigate complaints against a covered entity that assert retaliatory actions. In the past year, no complaints related to retaliatory or intimidating acts were filed with the CHPO by ESFCPCO patients. It appears that ESFCPCO is in compliance with the non-retaliation standards.

Uses and Disclosures Requiring Authorization

The OCR defines an authorization as a detailed document that gives covered entities permission to use PHI for specified purposes, which are generally other than treatment, payment, or health care operations, or to disclose PHI to a third party specified by the patient. An authorization must specify a number of elements, including: (1) a description of the PHI to be used and disclosed, (2) the person authorized to make the

use or disclosure, (3) the person to whom the covered entity may make the disclosure, (4) an expiration date, and (5) the purpose for which the information may be used or disclosed.

ESFCPCO management reported that workforce members are trained on and understand DMH Policy Number 500.1, *Use and Disclosure of Protected Health Information Requiring Authorization*, and are following the policy. ESFCPCO management indicated that because disclosures made by the facility are primarily for treatment, authorizations are rarely used.

We reviewed the DMH *Authorization for Request or Use/Disclosure of Protected Health Information* form, and verified it contains the HIPAA requirements. It appears that ESFCPCO is in compliance with HIPAA standards for uses and disclosures requiring authorization.

Accounting for Disclosures of Protected Health Information

The Privacy Rule gives patients the right to request and receive an accounting of all disclosures of their PHI made by the covered entity, with certain exceptions, for up to six years after the disclosure. The following disclosures of PHI are excluded from the accounting requirement: (1) to the patient, (2) for treatment, (3) for payment and health care operations, (4) for facility directories, (5) pursuant to authorization, (6) pursuant to a limited data set agreement, (7) to persons involved in the patient's care, (8) for correctional institutions, and (9) for certain law enforcement purposes. In addition, an accounting of disclosures' log must be maintained in each patient's medical chart.

ESFCPCO management reported that while they follow DMH Policy Number 500.6, *Accounting of Disclosures of Protected Health Information*, the facility does not make any non-routine disclosures, and all disclosures are for treatment purposes only. ESFCPCO management affirmed that they will track non-routine disclosures of PHI if any are made, and will maintain the logs in the patients' medical charts. ESFCPCO appears to be complying with the Accounting for Disclosures of PHI standards.

Minimum Necessary Rule

When using, disclosing, or requesting PHI from another covered entity, the Privacy Rule requires a covered entity to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. OCR provides covered entities with flexibility to address their unique circumstances, and make their own assessment of what PHI is necessary for a particular purpose.

Discussions with ESFCPCO management indicate that workforce members are aware of the minimum necessary standards. It appears that ESFCPCO is in compliance with the Minimum Necessary Rule standards.

HITECH Act Breach Notification

HHS' Breach Notification regulations require health care providers, health plans, and other covered entities to notify patients when their health information is breached. Specifically, health care providers and other covered entities must promptly notify affected patients of a breach, as well as the HHS Secretary and the media in cases where a breach affects more than 500 patients. Breaches affecting fewer than 500 patients will be reported to the HHS Secretary annually. The regulations also require business associates of covered entities to notify the covered entity of breaches at or by the business associate.

ESFCPCO management informed us that they trained their workforce members on DMH Policy Number 500.28, *Responding to Breach of Protected Health Information*, which provides guidelines and procedures for handling a breach or suspected breach of PHI. We reviewed the policy and determined that it provides proper guidance to workforce members. In addition, ESFCPCO did not report any breaches to the CHPO or OCR during the period 2010-2011. It appears that ESFCPCO is in compliance with the Breach Notification requirements.

Conclusion

Overall, our review indicates that ESFCPCO management is aware of and complying with HIPAA Privacy regulations. However, DMH's Compliance Division needs to work with ESFCPCO to address the deficiency noted in our review, and report any corrective action taken or pending to the HIPAA Compliance Office within 90 days from the receipt of this memorandum.

We thank DMH's Audit and Compliance Division and ESFCPCO managers and staff for their cooperation and assistance during this review.

Please call Linda McBride at (213) 974-2166 or Julia Chen at (213) 974-8315 if you have any questions.

WLW:RGC:GZ:LTM:JC

c: William T Fujioka, Chief Executive Officer
John F. Krattli, County Counsel
Robert Pittman, Chief Information Security Officer, Chief information Office
Judith L. Weigand, Compliance Officer, Department of Mental Health
Veronica Jones, Privacy Officer, Department of Mental Health
Audit Committee
Health Deputies